秘匿条件付きプロフィールマッチングプロトコルに関する考察

石黒 陽介 †　　面 和成 †

† 北陸先端科学技術大学院大学
923-1211 石川県能美市旭台 1 － 1
{s1410007,omote}@jaist.ac.jp

あらまし 近年，ユーザ同士のプロフィールをマッチングさせることにより，趣向の似た相手との交流を実現するソーシャルマッチングサービスが人気を高めている．一方で，マッチングサービスは個人情報を扱うので，その漏洩を防ぐために，情報を秘匿しつつマッチングさせることができる秘匿プロフィールマッチングプロトコルが研究されている．しかしながら，既存の方式では条件を考慮するようなきめ細かなマッチングができていない．本稿では，条件を満たしているならば，マッチングを行うといった階層的な処理を可能とする秘匿条件付きプロフィールマッチングプロトコルを提案する．本プロトコルはサーバが秘密情報を持たないように設計されているため，たとえサーバが攻撃を受けたとしても秘密鍵や参加者の個人情報が漏洩しない．

Consideration of Privacy-preserving Conditional Profile Matching Protocol

Yosuke Ishikuro†　　Kazumasa Omote†

†JAIST
Asahidai 1-1, Nomi-city, Ishikawa 923-1292, JAPAN
{s1410007,omote}@jaist.ac.jp

Abstract Social matching service which achieves interchanges between persons with similar interests have been popular by matching profiles each other in recent years. On the other hand, social matching service deals with personal data, so that privacy-preserving profile matching protocol, which can match user's profile while preserving personal data, has been studied for preventing its leakage. However, fine-grained matching as considering a condition has been not achieved in existing schemes. In this paper, we propose a privacy-preserving conditional profile matching protocol, which can deal with a hierarchical process such as the matching is performed when a condition is satisfied. In our protocol, if a server is attacked, there is not a leak of participant's secret key or personal data because our protocol is designed for a server not to hold such secret data.

1　はじめに

スマートフォンやタブレットなどのモバイル端末の普及により，ソーシャル・ネットワークは我々の生活にとって身近なものとなっている．それに伴い，ソーシャル・ネットワーク・サービス（SNS）も数多く生み出されている．それらサービスのなかには，ユーザの個人情報を扱うものも多く存在する．そのため，サービス事業

者は個人情報を適切に管理し，個人情報の漏洩や改ざん等の防止を徹底し，ユーザに安心感をもってもらうことが求められている．一方で，最近では，サービス等の向上のために，ユーザの個人情報を安全に利用することも求められている．そのため，個人情報を秘匿したままで安全に利用する技術が重要である．これにより，たとえサーバ上のデータがサイバー攻撃等によって漏洩したとしても，個人情報が漏れることを防ぐことができ，ユーザは安心してサービスを利用することができる．

個人情報を利用するソーシャル・ネットワーク・サービスのひとつに，ユーザ同士のプロフィールをマッチングさせることにより，似た趣向をもった相手との交流を実現することができるソーシャルマッチングサービスが人気を高めている．多くのソーシャルマッチングサービスで扱うユーザのプロフィールには，氏名や年齢，住んでいる地域などをはじめとした個人情報が含まれるが，現在利用されている多くのマッチングサービスにおいて，ユーザのプライバシーは考慮されていない．そこで，近年では，暗号技術を応用することにより，プロフィールを暗号化したままマッチングを行うことができる秘匿プロフィールマッチングプロトコルが研究されている．

しかしながら，既存の方式では，マッチングの条件を考慮するようなきめ細やかなマッチングができていない．すなわち，自身にとって受け入れらない趣向を相手がもっていたとしても，マッチングが成立してしまう恐れがある．例えば，ユーザ A が野球が好きな人とマッチしたいが，喫煙者とはマッチしたくないと思っているとする．一方，マッチングの相手 B は野球が好きだが，喫煙者である．本来ならば A は B とマッチしたくないのにも関わらず，既存の方式では「野球が好き」という部分がマッチしているため，マッチング成立という結果が出力されてしまう．

本稿では，このような問題に対処するために，条件を満たしているならばマッチングを行うといった，階層的なマッチング処理を可能とする秘匿条件付きプロフィールマッチングプロトコルを提案する．本プロトコルは，honest-but-curious なサーバを導入することにより，参加者 PC での暗号処理を最小限にする．また，本プロトコルはサーバが秘密情報を持たないように設計されているため，たとえサーバが攻撃を受けたとしても秘密鍵や参加者の個人情報が漏洩しない．

2 関連研究

Freedman ら [2] は，2004 に，Oblivious Polynomial Evalation (OPE) と加法準同型暗号用いて PSI プロトコルを初めて提案した．Kim ら [4] は，集合の要素として，OPE における多項式の解を使用する代わりに素数を使用することにより，参加者 PC の計算量を削減した．これにより，複数の回答を一つの暗号文に埋め込むことが可能となる．PSI プロトコルを基にした秘匿マッチングプロトコルには様々な方式が存在する．既存の方式について，大きく 2 つのタイプに分別することができる．ひとつは，プライバシーの強化に努めた方式，もうひとつはマッチング性能の強化に努めた方式である．

通常のマッチングでは，マッチした内容を結果として出力する場合が多い．一方で，マッチした内容を部分的に結果として出力することで，プライバシーの強化に努めた方式が存在する．[1] は，マッチした内容を明らかにせず，マッチした項目の個数のみを結果として出力する cardinality なマッチングを実現している．また，[5], [7] 及び [8] では，プライバシーレベルを設定し，レベルが上がるに従い，マッチング結果から得られる情報を少なくすることで，プライバシーを強化している．[9] は二人のユーザでマッチングを行ったとき，互いにマッチした項目の個数が同数の場合のみ，マッチング成功という結果を出力する．これにより，不当にマッチング結果を得ようとする攻撃者からプライバシーを守っている．

マッチング性能の強化を図った方式では，単にユーザ同士の興味をマッチングするだけでなく，より詳細なマッチングを実現している．[3] では，ユーザ自身が回答に重みを設けることによって，よりきめ細やかなマッチングを実現し

ている．[7] では，ユーザ自身の情報だけでなく，ユーザの友人の情報も利用することにより，より実生活に近い交流を実現することができるマッチングプロトコルを実現している．[6] では，[4] の方式をベースとして，多肢選択回答形式に対応したプロトコルを提案している．

以上のように，様々な秘匿マッチングプロトコルが提案されているが，どの方式もマッチングの条件を考慮するようなきめ細やかなマッチングができていない．

3 準備

3.1 要求事項

条件付きマッチングの実現

既存のマッチング方式では，相手が自身にとって受け入れらない趣向をもっていたとしても，それ以外の趣向が一致していればマッチングが成立してしまう恐れがある．そこで，本プロトコルでは，自身にとって受け入れられない特定の趣向をもった相手とのマッチングを行わないように，ある条件を満たすならば，マッチングを行う・行わないといった処理を可能とするマッチングプロトコルを実現する．

個人情報の安全管理

選択結果には参加者の個人情報が含まれる．そのため，サーバには選択結果を秘匿したまま保存しておくことが求められる．さらに，サーバが攻撃される可能性を考慮し，サーバは参加者や自身の秘密鍵を保持しないだけでなく，これら秘密鍵をサーバ上で一切使用しないことも必要である．これにより，サーバの安全管理が用意になる．

計算量の削減

既存のプロトコルの多くは，一つの質問に対し，一つの暗号文を生成する必要がある．これにより，質問の数が増えるに従い，暗号計算も必要となり，効率的でない．本プロトコルは，[4] や [6] のように集合の要素として素数を利用する．これにより，複数の質問に対して一つの暗号文で済むため，暗号処理の回数を削減することができ，計算量とメモリ消費量を削減できる．

3.2 Paillier 暗号

以下に，Paillier 暗号方式の各アルゴリズムを示す．

鍵生成アルゴリズム

$n = pq$ (p, q は大きな素数) と $g = (1 + \alpha n)\beta^n \bmod n^2$ ($\alpha, \beta \in \mathbb{Z}^*_{n^2}$) を計算し，公開鍵 (n, g) を出力する．また，秘密鍵として，$\lambda = lcm(p-1, q-1)$ を出力する．さらに，事前に $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$ を計算しておく．ここで，L は $L(u) = (u-1)/n$ と定義される．

暗号化アルゴリズム

メッセージ $M \in \mathbb{Z}_n$ に対して，乱数 $r \in \mathbb{Z}^*_{n^2}$ を選び，以下のようにして暗号文 $E(M)$ を計算する．

$$E(M) = g^M r^n \bmod n^2$$

復号アルゴリズム

暗号文 $c = E(M)$ に対して，以下のようにして平文を計算する．

$$\frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n = M$$

3.3 セキュリティモデル

セキュリティモデルとして，semi-honest モデルと malicious モデルの 2 種類がある．本稿では，semi-honest モデルを考える．semi-honest モデルとは，サーバ及び全ての参加者がプロトコルに従って振る舞うモデルのことである．また，サーバと参加者は結託しないものとする．このモデルの安全性では，下記のとおり，正当性と秘匿性を満たす必要がある．

- 正当性
  二人の参加者が各多肢選択のマッチング結果を正しく出力するなら，このプロトコルは正当性をもつ．

- 秘匿性
  マッチング結果に存在しない各参加者の多肢選択項目について何も知ることがないならば，このプロトコルは秘匿性をもつ．

4 秘匿条件付きプロフィールマッチングシステム

秘匿条件付きプロフィールマッチングシステムとは，二者の参加者間で各質問に対する選択を行い，各参加者が定めた条件を満たす相手とだけマッチングを行い，マッチしたものだけを得るシステムである．サーバ S 及び参加者 A，B は honest-but-curious なエンティティであると仮定する．つまり，S，A，B は，選択結果には関心はあるが，プロトコルに違反するような不正は行わないものとする．また，S は，A，B との結託を行わないことを前提とする．

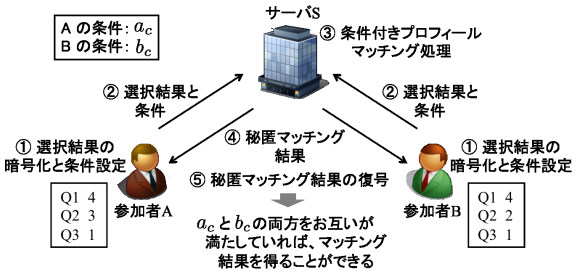

図 1: 秘匿条件付きプロフィールマッチングシステム

図 1 に，秘匿条件付きプロフィールマッチングシステムの概念図を示す．秘匿条件付きプロフィールマッチングシステムの基本的な手順は以下の通りである．

1. A，B は選択結果を暗号化し，それぞれが暗号化した結果を S に送信する．このとき，A 及び B は条件を設定し，それぞれ暗号文とともに送信する．
2. S は，条件付きプロフィールマッチング処理を暗号化したままで行い，その結果を A，B に返す．このとき，A, B それぞれから受け取った条件をマッチング処理に反映する．
3. A，B は秘匿マッチング結果をそれぞれで復号する．このとき，A の定めた条件を B が満たしている，かつ，B の定めた条件を A が満たしているならば，互いにマッチング結果を得ることができる．どちらか一方でも条件を満たしていなければ，正しいマッチング結果が出力されず，マッチング不成立となる．

5 提案方式

本章では，semi-honest な攻撃者に対して安全な秘匿条件付きプロフィールマッチングプロトコルを提案する．提案方式は基本的に [4][6] をベースとする．特に，[6] と同様に，サーバが参加者や自身の秘密鍵を持たない．さらに，本プロトコルでは，ユーザはマッチングのための条件を設定でき，その条件を満たしていない相手とはマッチしないプロフィールマッチング処理を行う．なお，サーバを設けることにより，参加者 PC の処理を最小限にする．

5.1 条件つきプロフィールマッチングへの対応

既存の方式では，自身にとって受け入れられない趣向を相手がもっていたとしても，それ以外の選択がマッチしていた場合，マッチングが成立する．この問題を解決する方法として，本稿ではマッチングの際に条件を設け，その条件を満たしているならば，マッチングを行うといった階層的なマッチング処理を扱えるようなマッチングプロトコルを提案する．

5.2 プロトコル詳細

図 2 をベースに，二者間の秘匿条件付きプロフィールマッチングプロトコルの詳細を述べる．本プロトコルは [4][6] をベースとするため，複数の質問に対して一つの暗号文で済む．この図では，$j(j = 1, ..., k)$ 番目の質問セットに対するプロトコルを記載している．質問セットとは，一つの暗号文に入れることができる質問の集合で

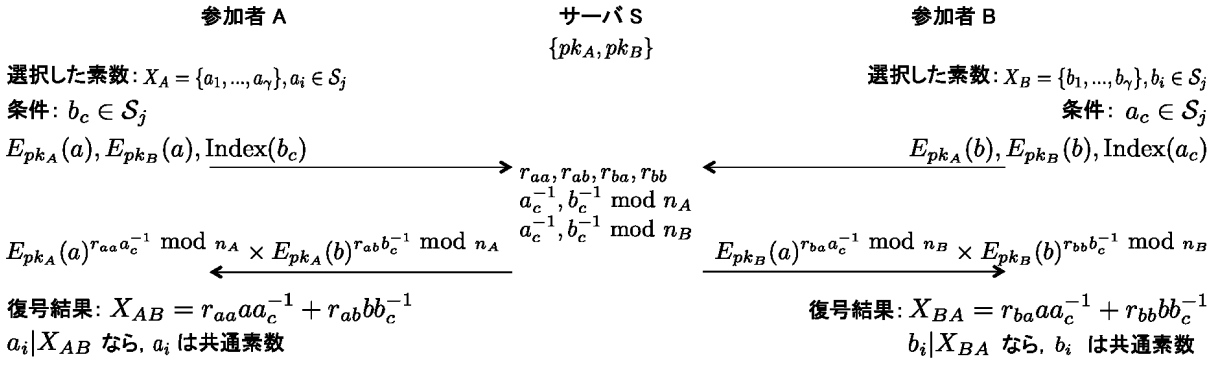

図 2: j 番目の質問セットに対する二者間の秘匿条件付きプロフィールマッチングプロトコル

ある．セット Q は全質問の集合を表し，Q_j は一つの暗号文にいれることができる j 番目の質問の集合 (質問セット) を表す ($Q_1 \cup Q_2 \cup \cdots \cup Q_k = Q, Q_{j_1} \cup Q_{j_2} = \emptyset, 1 \leq j_1, j_2 \leq k$)．参加者 A，B は選択結果に対応する素数 $X_A = \{a_1, ..., a_\gamma\} \in \mathcal{S}_j$, $X_B = \{b_1, ...b_{\gamma'}\} \in \mathcal{S}_j$ をそれぞれ選択するとする ($\mathcal{S}_1 \cup \mathcal{S}_2 \cup \cdots \cup \mathcal{S}_k = \mathcal{S}, \mathcal{S}_{j_1} \cup \mathcal{S}_{j_2} = \emptyset, 1 \leq j_1, j_2 \leq k$)．$\mathcal{S}_j$ は一つの暗号文に入れることができる j 番目の質問セットで使われる t ビットの素数の集合を表し，公開される．また，$|\mathcal{S}_j|$ は j 番目の質問セットにおける選択可能な素数の数を表す．選択結果は素数の積で表され，A，B の結果をそれぞれ $a = \prod_{i=1}^{\gamma} a_i$, $b = \prod_{i=1}^{\gamma'} b_i$ と表す．

さらに， A が設定する条件を $b_c \in \mathcal{S}_j$，B が設定する条件を $a_c \in \mathcal{S}_j$ と表す．条件に関して，A が設けた条件 $b_c \in \mathcal{S}_j$ を B が選択していなければ B とマッチングしない，ということを意味する．$a_c \in \mathcal{S}_j$ についても同様である．ただし，条件の設定はどちらか一方だけでも，問題なくマッチングは行われる．A と B は対照的であるため，ここでは A がマッチング結果を得る手順を主に説明する．なお，A と B は認証された通信路を利用することを仮定する．また，[6] と同様に，A と B は直接通信を行わない．

1. S は，k 個の質問セットに対応して，集合 $\{\mathcal{S}_1, ..., \mathcal{S}_k\}$ を選択する．
2. A，B は，加法準同型暗号を設定し，それぞれ自身の公開鍵 pk_A, pk_B を公開する．
3. A は，自身と B の公開鍵のそれぞれを用いて，自身の選択結果を暗号化することによって $E_{pk_A}(a)$ と $E_{pk_B}(a)$ を求める．さらに，A は条件 b_c を決定し，暗号文とともに b_c のインデックスを S に送信する．B も同様に，自身の公開鍵と A の公開鍵を使って選択結果を暗号化し，自身の設定した条件 a_c のインデックスとともに S に送信する．
4. S は，乱数 $r_{aa}, r_{ab}, r_{ba}, r_{bb}$ を生成する．これらの乱数はメッセージ空間のパディングに使用される．参加者 A, B の条件数をそれぞれ λ_A, λ_B とすると，乱数のサイズはそれぞれ，$|r_{aa}| = |n_A| - |Q_j|t + \lambda_B t - 1$, $|r_{ab}| = |n_A| - |Q_j|t + \lambda_A t - 1$, $|r_{ba}| = |n_B| - |Q_j|t + \lambda_B t - 1$, $|r_{bb}| = |n_B| - |Q_j|t + \lambda_A t - 1$ となる．さらに，S は A 及び B から受け取った条件のインデックスから，それに対応する値を取り出す．そして，取り出した値の逆元をそれぞれ n_A の元で計算する．すなわち，$b_c^{-1}, a_c^{-1} \bmod n_A$ を計算する．B に対しても，n_B の元で A, B の条件の逆元 $b_c^{-1}, a_c^{-1} \bmod n_B$ を計算する．そして，生成した乱数と計算した逆元を使って，次の式 (1) を計算する．

$$\begin{aligned} & E_{pk_A}(a)^{r_{aa}a_c^{-1}} \times E_{pk_A}(b)^{r_{ab}b_c^{-1}} \\ &= E_{pk_A}(r_{aa}aa_c^{-1} + r_{ab}bb_c^{-1}) \\ &= E_{pk_A}(X_{AB}) \end{aligned} \tag{1}$$

その後， S は，式 (1) の値を A に送信する．このとき，$X_{AB} = r_{aa}aa_c^{-1} + r_{ab}bb_c^{-1}$,

$X_{BA} = r_{ba}aa_c^{-1} + r_{bb}bb_c^{-1}$ と表される．

5. A は，式 (1) の値を復号して X_{AB} を得る．
6. A は，自身の選択結果を示す全ての素数に対して，マッチング検証を行う．すなわち，$a_i|X_{AB}$ $(i = 1, ..., \gamma)$ をチェックする．これが真であるならば，a_i は共通素数ということであり，偽であるならば a_i は共通素数ではないということになる．ただし，このとき，A の定めた条件を B が満たしている，かつ，B の定めた条件を A が満たしていれば，互いにマッチング結果を得ることができるが，どちらか一方でも条件を満たしていなければ，正しいマッチング結果を得ることができず，マッチング不成立となる．B も同様である．

なお，二者間のプロトコルを並列で動作させて，m 人におけるプロトコルを容易に構築できる．

5.3 条件設定のメカニズム

本節では，提案プロトコルにおける条件設定のメカニズムについて述べる．まず，条件に関して，参加者は自身と相手が設定した条件を同時に満たしている場合にのみ互いに正しいマッチング結果を得ることができるというものである．すなわち，A の条件が b_c，B の条件が a_c の場合，正しいマッチング結果を得るためには，A が a_c，B が b_c を選択していなければならない．もし，どちらか一方でも条件を満たしていなければ，互いにマッチング結果を得ることはできない．このメカニズムについて，具体例を用いて示す．

参加者 A は自身の回答として，$a = xyz$，参加者 B は $b = wxyz$ を持つとする．x, y, z, w はそれぞれ選択結果に対応する素数を表す．このとき，A は条件として $b_c = x$，B は条件として，$a_c = y$ を設定する．この場合，A は a_c，B も b_c を選択しているため，正しくマッチング結果が出力される．すなわち以下となり，復号後の検証の結果，z を共通素数として求めることができる．

$$
\begin{aligned}
&E_{pk_A}(a)^{r_{aa}a_c^{-1}} \times E_{pk_A}(b)^{r_{ab}b_c^{-1}} \\
&= E_{pk_A}(r_{aa}xyzy^{-1} + r_{ab}wxyzx^{-1}) \\
&= E_{pk_A}(r_{aa}xz + r_{ab}wyz)
\end{aligned}
$$

これにより，A, B 間のマッチングでは，z が示す質問についてマッチしたということが判る．

一方で，B の条件が $a_c = w$ のとき，以下のように計算される．

$$
\begin{aligned}
&E_{pk_A}(a)^{r_{aa}a_c^{-1}} \times E_{pk_A}(b)^{r_{ab}b_c^{-1}} \\
&= E_{pk_A}(r_{aa}xyzw^{-1} + r_{ab}wxyzx^{-1}) \\
&= E_{pk_A}(r_{aa}xzw^{-1} + r_{ab}ywz)
\end{aligned}
$$

この場合，A が B の条件を満たしていないため，B の条件 $a_c = w$ の逆元 w^{-1} が残ったままになる．これにより，メッセージ空間 n_A 上で桁あふれが高い確率で生じてしまい，共通素数を求めることができなくなる．すなわち，A, B のマッチングは成立しない．

6 評価

6.1 安全性

6.1.1 正当性

Theorem 1. (正当性). 提案プロトコルはマッチング結果を正しく出力する．

Proof. まず，$x \in X_A \cap X_B$ と仮定する．このとき，x は a かつ b を割り切る．ゆえに，x は $X_{AB} = r_{aa}a + r_{ab}b$, 及び $X_{BA} = r_{ba}a + r_{bb}b$ の両方を割り切る．したがって，各参加者は x が共通選択結果であることを知る．次に，$x \notin X_A \cap X_B$ と仮定する．このとき，(1) どちらか一方だけに含まれる．(2) どちらにも含まれない，の 2 つのケースが考えられる．しかしながら，(1), (2) のどちらのケースにおいても，P_1 の確率で，$X_A \cap X_B$ に x が誤って共通素数として存在する (ただし，P_1 は 6.3 節の式 (2) を参照)．ゆえに，本プロトコルは式 (2) の確率で正当性を保証することができる． □

表 1: 効率性の比較

方式	計算量	通信量
[4]	$\mathcal{O}(\|Q\|)$	$\mathcal{O}(\|Q\|)$
[7]	$\mathcal{O}(\|Q\|^2)$	$\mathcal{O}(\|Q\|)$
[8]	$\mathcal{O}(\|Q\|)$	$\mathcal{O}(\|Q\|)$
提案方式	$\mathcal{O}(\|Q\|)$	$\mathcal{O}(\|Q\|)$

表 2: 各処理における演算処理時間の 10 回平均

タブレット端末			サーバ PC
暗号化 (2 回分)	復号 (1 回分)	マッチング検証	マッチング処理
165ms	51.3ms	7.92ms	30.6ms

6.1.2 秘匿性

次の Theorem 2 は，提案プロトコルが秘匿性を有していることを示す．

Theorem 2. (秘匿性)．攻撃者は，正直な参加者と共通の選択項目以外で正直な参加者の選択について何も有益な情報を得ることができない．

Theorem 2 に関する証明については，[6] と同じであるため，ここでは省略する．

6.2 効率性

本節では，各参加者のタブレット端末及びサーバ PC の計算量及び通信量について評価する．また，各処理における実装評価を行う．

6.2.1 通信量及び計算量

二者間の秘匿条件付きプロフィールマッチングプロトコルにおいて，参加者は各質問に対して 2 つの暗号文を送受信する．提案方式では各参加者が送受信する暗号文の通信回数は $4|Q_j|$ となる．ゆえに，提案方式の通信量は $\mathcal{O}(|Q|)$ で表される．

計算量については，最も処理が重いべき乗剰余の回数で評価する．Paillier 暗号では，暗号化にべき乗剰余が 2 回必要であり，復号にべき乗剰余が 1 回必要である．提案方式では，各質問に対して 2 回の暗号化と 1 回の復号が必要となるため，各参加者のべき乗剰余回数は $5|Q_j|$ 回となる．ゆえに，提案方式の計算量は $\mathcal{O}(|Q|)$ で表される．

表 1 は提案方式と既存方式の効率性の比較である．比較対象には，提案方式と同様，マッチングの結果としてどの項目がマッチしたかを知ることができる既存方式を選択している．これより，提案方式では，計算量，通信量が共に低いことが明らかになった．

6.2.2 実装評価

提案方式の実装評価を行う．評価に関しては，サーバ PC 及び参加者のタブレット端末における演算処理時間を測定する．

実装に関して，サーバ PC と参加者のタブレット端末に分けてそれぞれ評価を行う．サーバ PC は，CPU が Intel Core i5 1.4GHz, メモリが 8GB RAM, OS が OS X Yosemite 10.10.4 である．参加者のタブレット端末は NEXUS7, CPU は Qualcomm Snapdragon S4 Pro 1.5GHz, メモリが 2GB RAM, OS が Android 4.4.2 である．なお，本実装は JAVA で行った．

具体的なパラメータに関して，マッチングの失敗確率が 2^{-20} 以下で正当性を保証すると仮定し，表 3 より $t = 28$ ビットの素数を用いる ($|Q_j| = 30$)．ここでは，参加者は各質問に割り当てられた 5 個の選択肢に対して，単一回答を行うこととする．

演算処理時間に関して，タブレット端末上では 2 回分の暗号化，1 回分の復号，及びマッチング検証の処理時間，サーバ PC 上ではマッチングの処理時間を計測した．表 2 は各処理における演算処理時間 (10 回平均) を示している．

6.3 マッチングの失敗確率

表 3 は t を変化させた場合に，一つの暗号文に入れることができる質問の個数 $|Q_j|$ と，そのマッチングの失敗確率を示している．本プロ

表 3: t を変化させた際の $|Q_j|$ 及びマッチングの失敗確率 P_1

t	$\|Q_j\|$	P_1
25	34	5.07×10^{-6}
26	33	2.46×10^{-6}
27	31	1.15×10^{-6}
28	30	5.59×10^{-7}
29	29	2.70×10^{-7}
30	28	1.30×10^{-7}
31	27	6.29×10^{-8}

トコルでは，正しいマッチング結果が出力されない場合がある．例えば，$x \notin X_A \cap X_B, x \in \mathcal{S}_j$ にもかかわらず，x が誤って A と B の共通素数になるならば，正しいマッチング結果が出力されない．式 (2) の通り，P_1 は $\mathcal{S}_j$ に含まれる t ビットの素数の全候補に対して，それらの素数が $X_A \cap X_B$ に共通素数として誤って存在する確率であり，マッチングの失敗確率となる．

$$P_1 = 1 - \left(1 - \frac{1}{2^t}\right)^{|\mathcal{S}_j|} \tag{2}$$

7 まとめ

本稿では，semi-honest な攻撃者に対して安全である，秘匿条件付きプロフィールマッチングプロトコルを提案した．本方式では，参加者自身が条件を設定できることにより，既存の方式において生じる恐れのある参加者同士のミスマッチを防ぐことに成功している．今後の課題としては，マッチング情報を限定するプライバシーレベルの設定や条件の秘匿など，プライバシーの強化が挙げられる．

参考文献

[1] F. Abbas, Ubaidullah, R. Hussain, H. Eun, and H. Oh, “A Trustless Broker Based Protocol to Discover Friends in Proximity-Based Mobile Social Networks”, *WISA 2014*, pp.216–227, 2014.

[2] M.J. Freedman, K. Nissim and B. Pinkas, “Efficient Private Matching and Set Intersection”, *EUROCRYPT 2004*, pp.1–19, 2004.

[3] D. He, Z. Cao, X. Dong, and J. Shen, “User Self-controllable Profile Matching for Privacy-preserving mobile Social Networks”, *IEEE ICCS 2014*, pp.248–252, 2014.

[4] M. Kim, H.T. Lee, and J.H. Cheon, “Mutual Private Set Intersection with Linear Complexity”, *WISA 2011*, pp.219–231, 2011.

[5] M. Li, S. Yu, N. Cao, and W. Lou, “Privacy-Preserving Distributed Profile Matching in Proximity-Based Mobile Social Networks”, *IEEE Trans. on Wireless Communications*, vol.12, no.5, pp.2024–2033, 2013.

[6] 面和成，“秘匿多肢選択マッチングプロトコルの提案と評価”，*Computar Security Symposium 2014*, pp.659–666, 2014.

[7] A. Thapam, M. Li, S. Salinas, and P. Li, “Asymetric Social Proximity Based Private Matching Protocols for Online Social Networks”, *IEEE Trans. on Parallel and Distributed Systems 2014*, vol.26, no.6, pp.1547–1559, 2014.

[8] R. Zhang, Y. Zhang, J.S. Sun, and G. Yan, “Fine-grained Private Matching for Proximity-based Mobile Social Networking”, *IEEE INFOCOM 2012*, pp.1–9, 2012.

[9] H. Zhu, S. Du, M. Li, and Z. Gao, “Fairness-Aware and Privacy-Preserving Friend Matching Protocol in Mobile Social Networks”, *IEEE Trans. on Emerging Topics in Computing 2013*, vol.1, no.1, pp.192–200, 2013.